* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] The sensor equipment which detects the physiological description of the user of a device (BM), for example, a fingerprint, in the device for electronic equipment, for example, information processing, or a communication link (SE), b) The data processor for which it asks from the physiological description which had the information (FPAUTINF) used for a user's authentication detected (DE), c) A means to input the information (AUTINF) used for authentication through the input unit (EE) which inputs information, and this input unit, d) -- or [having asked] -- or the electronic equipment characterized by what it has test equipment (PE) which inspects the inputted authentication information, and releases the function of a device to the user of this ** when inspection is effective for.
[Claim 2] Said data processor (DE) is a device according to claim 1 constituted so that identically to the authentication information (FPPIN) asked for the authentication information (PIN) inputted through an input unit for inspection of effective authentication from the physiological description of the user who has authority.
[Claim 3] Said data processor (DE) is the device according to claim 1 or 2 which can use the multiple processes (M1, ..., Mn) which search for the information (FPAUTINF1, ..., FPAUTINFn) used for authentication of the user of this ** from a user's detected physiological description.
[Claim 4] Said data processor is a device according to claim 3 as which a desired process is made to choose from the physiological description among the multiple processes which search for authentication information to the user who has authority.
[Claim 5] The device given [to claims 1-4] in any 1 term which has a means to display the authentication information (FPAUTINF) searched for from a user's physiological description.
[Claim 6] The user has the means which attests by using the physiological description of a proper for a user, or inputting authentication information through an information input unit. In the 1st case, sensor equipment detects a user's physiological description. How to attest the device user characterized by what it inspects with test equipment in quest of the information used for authentication from the detected physiological description, and the authentication information which the user inputted through the input unit in the 2nd case is inspected for with the same test equipment.
[Claim 7] a) How to attest the device user according to claim 6 who has the step which asks for a feature vector from the measurement data of sensor equipment, the step which quantizes a vector from the feature vector b Called for, and the step which inspects the authentication information corresponding to the result of quantization of c vector.

[Translation done.]

* NOTICES *

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
Before using, very various electronic equipment by which a user has to perform authentication thru/or OSEN Tiffe KESHON is known. The main example is, the computer (information management system) of various configurations, communication equipment, for example, a mobile phone etc., etc. There are some which are generally protected by the password as opposed to the unauthorized use in these devices. Other devices have protected only the predetermined function by for example, the so-called personal identification number (PIN) to unlawful access. Predetermined data or protection of access to service also belongs to this. That is right, even when this is not used by the device and used by a computer network or the communication network.
[0002]
The input of the authentication information on the format used frequently today is an input through the keyboard of a device. The informational justification inputted after the input, as a result the authority of the user who performed the input are inspected with the test equipment of a device, a computer network, or a communication network. In the mobile phone based on GSM specification, this is performed by inspecting whether inputted PIN suits the information memorized by the SIM card using the data processor on the so-called SIM card of a device. In suiting, a mobile phone becomes usable by the SIM card. Where PIN was not memorized and is locked in a device based on GSM specification, when the SIM card memorizes, the security of the customer of a telephone goes up.
[0003]
The technique which can attest a user in the form of others from before for a while is used. This technique is based on detecting the physiological description of a proper by the special sensor to a user. This main example is a fingerprint detection sensor. Another physiological description is the property of the retina tissue the human being's eyes', or human being's voice, and these are similarly used by several sorts of devices.
[0004]
Usually, when the description detected by the sensor is compared with the known description of the user who has authority and is fully in agreement with a device or the data processor of a communication network, access to the function of desired service, required data, or the selected device is released.
[0005]
It is significant if authentication of the two above-mentioned formats combines mutually by the device of some types. For example, it is more desirable a user not only can to use a telephone by the fingerprint sensor, but to be able to carry out the share of PIN to other persons, or to be able to use in a mobile phone, so that it can use within the limits of the authority to which the device is given by the SIM card of a proper. The authentication which furthermore minded the fingerprint generates an error accidentally, or becomes activation impossible. This is the case where a user's hand is dirty or the user has stuck the glove. It is that desirable one (or thing which is the need) can be attested from these reasons or other reasons by the technique from which one person or two or

more users of a device differ. Physiological authentication is performed together with authentication by the PIN input in this case. In the mobile phone based on GSM specification, this specification has defined the authentication means by the PIN input beforehand compulsorily.

[0006]

The above-mentioned situation shows that the conventional physiological authentication process is impossible in the mobile phone based on GSM specification. It is because authentication by PIN using a SIM card is surely required from the reason of compatibility over GSM specification. As a means which looks possible for the time being, PIN is memorized in a device, and this is eliminated although it is possible to transfer PIN memorized in accordance with the detected fingerprint and the fingerprint with which the user who has authority was memorized when inspection is effective to a SIM card, and to inspect it. It is because it is forbidden by GSM specification from the reasons of security to memorize PIN in somewhere else other than the interior of a SIM card in a mobile phone. Physiological authentication is taken into consideration as a security means additional in this case. However, such an additional security means is unnecessary if it carries out from the high safety of authentication by the PIN input, and many users cannot accept it easily and should sense it.

[0007]

The technical problem used as the foundation of this invention is offering the technical thought which makes possible combination of a physiological user's authentication, and authentication by the PIN input also in the mobile phone of GSM specification or a similar case, and enables it to fully utilize authentication of each format. It has the option whether a user wants to use authentication of which format. However, it can have a means by which the user (for example, owner of a device) chosen especially can adjust logic AND association of two authentication formats in a device. This technical problem is solved by the claim by the device or approach of a publication.

[0008]

In this invention, a user's physiological description is detected by sensor equipment and the information used for authentication is searched for using a mathematical process from the detected physiological description. Authentication information arises in the culmination which evaluates the physiological description by this, and this information is inspected with the same test equipment as inspecting the authentication information which the user inputted through the information input device (for example, keyboard). In the easiest case, the result of assessment of a fingerprint becomes the same thing as PIN which the user inputted through the keyboard. However, this PIN is calculated from a user's physiological description detected by sensor equipment rather than is memorized by the device.

[0009]

According to the format of evaluating the physiological description detected by sensor equipment, authentication of this format does not need to become equivalent to the result of authentication through the input of a keyboard, and it becomes unnecessary to change the usual interface which inspects the validity of authentication. It is not necessary to change a certain protocol standardized especially. The two technique of authentication can be used in [it is satisfactory and] juxtaposition. A user can choose two technique freely in any condition at any time. It can also constitute so that authorization may be given only to the user to whom the two authentication technique passed effectively, of course using AND association.

[0010]

Below, this invention is **(ed) in the advantageous example and explained at a detail using drawing.

[0011]

The example of this invention by which all approaches and equipment are accumulated into the device is shown in drawing 1 .

[0012]

The example of this invention to which test equipment exists in a device is shown in drawing 2 .

[0013]

The example of this invention on which the display which displays authentication information is accumulated by the device is shown in drawing 3 .

[0014]

An example typical and important for this invention moreover is a mobile phone based on GSM specification, and this uses a fingerprint sensor for a user's authentication. This fingerprint sensor is the special example of the sensor equipment SE shown in drawing 1 . The user of Device EG puts a finger on this fingerprint sensor, and if it is standing by attesting inputs of a device, such as PIN, SuperPIN, or PIN2 (it being selectively dependent on a manufacturer), a fingerprint sensor detects the suitable physiological description BM of the user of this **, and sends this out to data-processor DE.

[0015]

In the case of a GSM mobile phone, this data processor is with the processor already prepared in the mobile phone, and the software which operates on this processor. however, on the other hand, the special software with which sensor equipment or -- general -- is used through the processor unit of a proper, and a fingerprint sensor manages fingerprint recognition on this processor unit operates. Thereby, the data processor is incorporated in sensor equipment completely selectively in the range of this invention. As for the fingerprint recognition itself, like other technique of recognizing the physiological description, since it is fully common knowledge at this work engineer, the implementation gestalten (and integration of partitioning with a subsystem, or a well-known hardware module), i.e., the various configurations, of a data processor, about this part, especially a problem does not have them in implementation of the security of this invention.

[0016]

According to this invention, a data processor searches for the information which was suitable for a user's authentication from the detected physiological description. It is PIN (or PIN2 in addition to this) memorized in the condition of having been locked on the SIM card of the user regarded as this having authority in the easiest case. This PIN is handed over and inspected to a SIM card, as the user inputted through the keyboard (information input unit) of a mobile phone. Next, to this work engineer, the inspection process set to well-known GSM specification operates within the test equipment (a SIM card, equipment connected with the data processor of a device by the case) of a mobile phone. When the authentication information FPAUTINF is in agreement with PIN memorized on the right case, i.e., a SIM card, the functions (for example, network access etc.) of the device protected according to authentication are released.

[0017]

The important advantage of the means of above-mentioned this invention is that the fingerprint recognition section hands over a user's PIN to a SIM card, when the user has authority. It is because it is not necessary to change the security protocol of GSM specification at all by this. This advantageous property does not exist in a means by which it is thought that others are fundamental. make it any -- with other means, the input of additional PIN through a keyboard is needed, or evasion thru/or modification of GSM specification is needed. The input of additional PIN through a keyboard is effective only when taking into consideration as an additional security means which added fingerprint recognition to the PIN input.

[0018]

Of course, such additional authentication is possible also by this invention. In this case, it is not necessary to transmit the authentication information searched for from sensor data to a SIM card. Instead, PIN which was intentionally mistaken, for example may be transmitted to a SIM card, or an input error, interruption, others of an input, etc. may be simulated. On the other hand, a SIM card newly requires an PIN input. In accordance with PIN asked for inputted PIN, when interexchangeable, data-processor DE transmits this PIN to a SIM card, and release is permitted according to this.

[0019]

PIN calculated from sensor data, of course may not necessarily be the same as that of PIN of a SIM

card. By above-mentioned specification or other above-mentioned devices, when a suitable security protocol grants a permission each time, test equipment can inspect whether these suit mutually using two different authentication information.

[0020]

When there is authentication information FPAUTINF calculated from sensor data only by one authentication (namely, authentication simultaneous with an PIN input or authentication independent of this) by sensor data, by other devices which are not based on GSM specification, it may differ from the authentication information AUTINF inputted through the keyboard, but if two information directs the user who has authority, these will recognize test equipment to conform simultaneously.

[0021]

All mathematical simulation (function) is fundamentally taken into consideration as a count process over the authentication information FPAUTINF acquired from the physiological description BM, and the authentication (generally it encoded with alphabetic character) information AUTINF on other formats is assigned to a fingerprint or other physiological descriptions BM. The following conditions must be satisfied here. namely, a -- the same authentication information FPAUTINF fully draws from the similar physiological description BM -- having -- b -- authentication information FPAUTINF which is different from the fully different physiological description BM draws -- having -- c -- for an inaccurate user, what the authentication information FPAUTINF is searched for for from the physiological description BM or the information of this description BM (for example, it guesses) is an impossible thing substantially.

[0022]

It guarantees that Conditions a fully have fingerprint recognition by the low bust also to a small noise. Otherwise, it is because the rate that the user who has authority is refused becomes very high. Conditions b are established so that a different user's fingerprint may derive the authentication information FPAUTINF various by the probability high enough to this. The meaning of Conditions c is clear.

[0023]

The various mathematical simulation which is satisfied with this contractor (there is some of appropriateness by the case) of this demand is common knowledge. The simulation which has these properties is given by the so-called vector quantization. About the technique of common knowledge to this contractor, the individual reason considered to be here required for an understanding of this invention outside is not explained.

[0024]

It is premised on the physiological description detected by sensor equipment being first moved to the so-called format of a feature vector in case this technique is used for the object of this invention. This assumption does not turn into any definition actually, either. It is because sensor data are expressed as n groups who were always able to set in order n measurement data (feature vector). A feature vector forms n-dimensional space. In this space, the set (code book vector) of a pattern vector exists, and an interval scale (degree of the resemblance to the physiological description) is specified. The cel in space exists to each pattern vector, this cel ****s in each feature vector in a cel, and the pattern vector is prescribed by by being the cel of the pattern vector which exists in a degree within the limits of the interval scale of this **.

[0025]

The information for which it was fundamentally suitable in authentication is assigned to each pattern vector. Exact authentication information (for example, true PIN) is assigned to one pattern vector. If it asks for the pattern vector which exists in a degree to the predetermined feature vector which ****s to the detected sensor data so that clearly from the above-mentioned explanation, when the user of this ** has authority, exact information (true PIN) is drawn, and when that is not right, the mistaken authentication information will be sent out. The error rate of this process can be optimized when it is guaranteed that the feature vector relevant to the physiological description of the user

who has authority is one of the pattern vectors. This is attained by fitting this system to the physiological description of the user who has authority in an initialization phase (formation of code book adaptation).

[0026]

Vector quantization is not the only technique which can be used in relation to this invention. Other technique of not explaining to this contractor here can be enforced.

[0027]

Originally calculating the authentication information FPAUTINF by vector quantization from a user's physiological description is connected with "storage of PIN" by the device (if based on this description). It is because the possible authentication information FPAUTINF is fundamentally assigned to each pattern vector of a code book. However, this is actually (except for one user's, i.e., the user who has authority, feature vector) suitable for authentication in almost no cases. Although it is got blocked, for example, all possible PIN is ideally memorized in PIN of the alphabetic character of 5 figures and a pattern vector is assigned to every one each of these, only when a pattern vector is fully detected by accuracy, addressing can be carried out to appropriate PIN within a sensor. The number of possible PIN will become large too much, and it will become impossible therefore, to find out exact PIN in spite of "memorizing in the device" except the user who has the exact physiological description. Such a situation is not taken into consideration when memorizing PIN to a device by specification is forbidden.

[0028]

Memorizing PIN to a device is not permitted by GSM specification. However, the need of changing PIN is produced frequently. This is the case where PIN is known by the 3rd person etc. However, it is that which calculates PIN from a fingerprint in this invention (that is, it calculates), and unless exchange of a fingerprint or other physiological descriptions is possible, this is impossible first. If a means to change PIN is still given to a user, it constitutes so that it may replace only with one count process and all sets of this kind in a device of process can be equally used according to the advantageous operation gestalt of this invention. The consecutive number is assigned to each count process and the user who has authority to this can change the process to be used at any time. Since each processes M1, ..., Mn over the same fingerprint BM calculate other PIN (FPAUTINF1, ..., FPAUTINFn), it chooses whether a user makes much PIN calculate in which process.

[0029]

The example of this invention is realizable similarly with vector quantization. Not only a code book but two or more code books of a pattern vector are prepared here. Each code book has the predetermined number and is selectable through this number. Probably it depends for other processes on a parameter. In this invention, other mathematical simulation is formed by changing this parameter. If the dependency of a parameter is fully complicated, as for modification of authentication information, a guess will become impossible even if it changes a parameter actually. The neural network (the so-called multilayer perceptron) of a predetermined type is suitable for realizing this kind of simulation. With the means based on this neural network, actually, anywhere, PIN is not memorized as a notation sequence but is only memorized by network architecture as a weighting multiplier (in the condition of having been locked suggestively).

[0030]

Especially in this example of this invention, it is taken into consideration from a viewpoint for which the sequence of the password with which many persons differ is needed to the thoroughly different object or a thoroughly different device. It should become increasingly difficult to care about many passwords. When using multiple processes M1, ..., Mn (mathematical simulation) for count from the only feature vector (sensor data aggregate) of two or more authentication information (FPAUTINF1, FPAUTINF2), the problem at the time of detecting the physiological description which a user cannot do at **** of a proper is reduced by the suitable sensor.

[0031]

What is necessary is just to input the index of this kind of process in the context only prepared in a user's actuation front face, in order to choose a predetermined process. Thereby, a data processor can constitute suitably for every software.

[0032]

Of course, two or more persons' physiological description is also combinable with one or more right PIN. When the device is combined only with one person as an exception (i.e., when only one SIM card is used for accuracy), release can be additionally combined with other security devices, for example, the code of a device etc. According to this invention, the flexibility of each format, high safety, and the compatibility over specification are acquired here.

[0033]

When changing PIN, in the another advantageous example of this invention, the display for presenting of authentication information is prepared especially. Since this kind of displays are this kind of devices [many] and have already existed since the start, this can be used for this object. If it is going to change the authentication information AUTINF (for example, PIN) which the user inputted through the keyboard into the information which suits a SIM card, in some count processes, combination of the figure of all possible notations cannot use it as PIN by the case. For example, it is because it is smaller than the number of all PIN in which a code book is possible. This case is enough to assign PIN to a pattern vector and change PIN corresponding to an individual pattern vector if the parameter of the count process used is changed (for example, modification of a code book number or modification of a neural network's parameter). If PIN on a SIM card (or PIN which should generally be inputted) is not known after that, it becomes impossible to change in this semantics. And this is required because of the further utilization to the technical problem of this invention. The user who has authority can be told about changed PIN by making the display of a device give a short-time indication only once suitably, advantageously, after changing PIN. Other means (for example, show new PIN later) are possible.

[0034]

Of course, this invention is not limited to a mobile phone, for example, the mobile phone based on GSM specification. It is not difficult for this contractor to realize this invention in other devices or alien systems based on the above-mentioned explanation, either.

[0035]

Especially this invention is not limited only to the case where the inspection unit PE is accumulated into the device. The important example of a device is shown in drawing 2 , a device is connected with other at least one device through a communication network, and test equipment also exists in a network here. Moreover, the part which manages calculating the authentication information FPAUTINF from a part of data processor or data processing unit DE BM, i.e., a user's physiological description, does not necessarily need to exist in a device, either. Of course, the device does not need to have the accumulated sensor equipment SE or the accumulated keyboard EE. It is also clear that equipment may be connected to a device in the form of an external module. The example of this invention should be protected by the claim of an approach.

[Brief Description of the Drawings]

[Drawing 1]

All approaches and equipment are drawings showing the example of this invention accumulated into the device.

[Drawing 2]

All approaches and equipment are drawings showing the example of this invention accumulated into the device.

[Drawing 3]

The display which displays authentication information is drawing showing the example of this invention accumulated by the device.

[Translation done.]

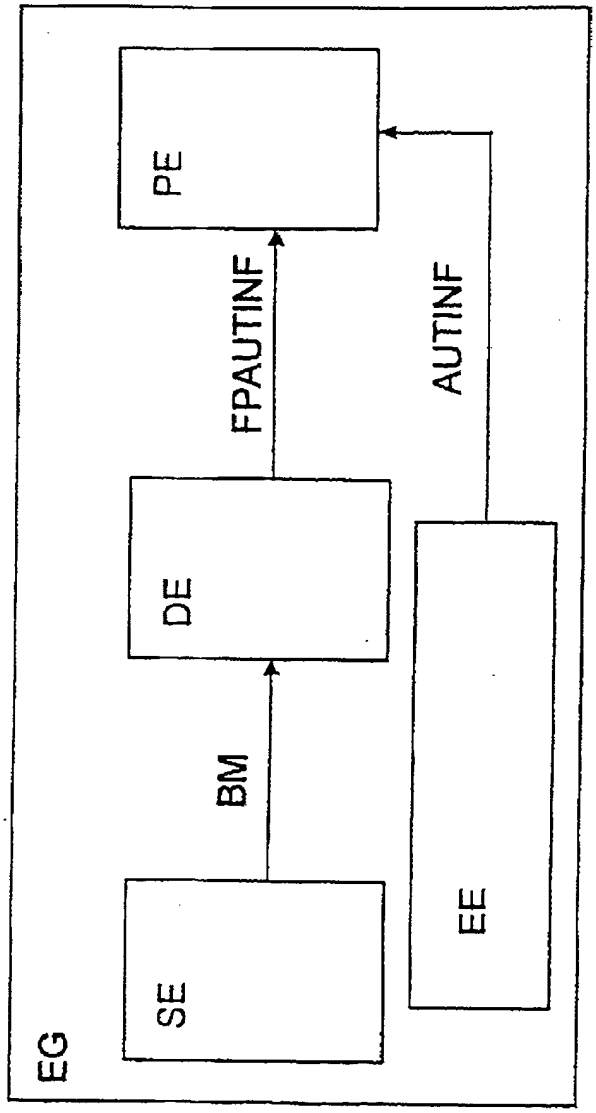
* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

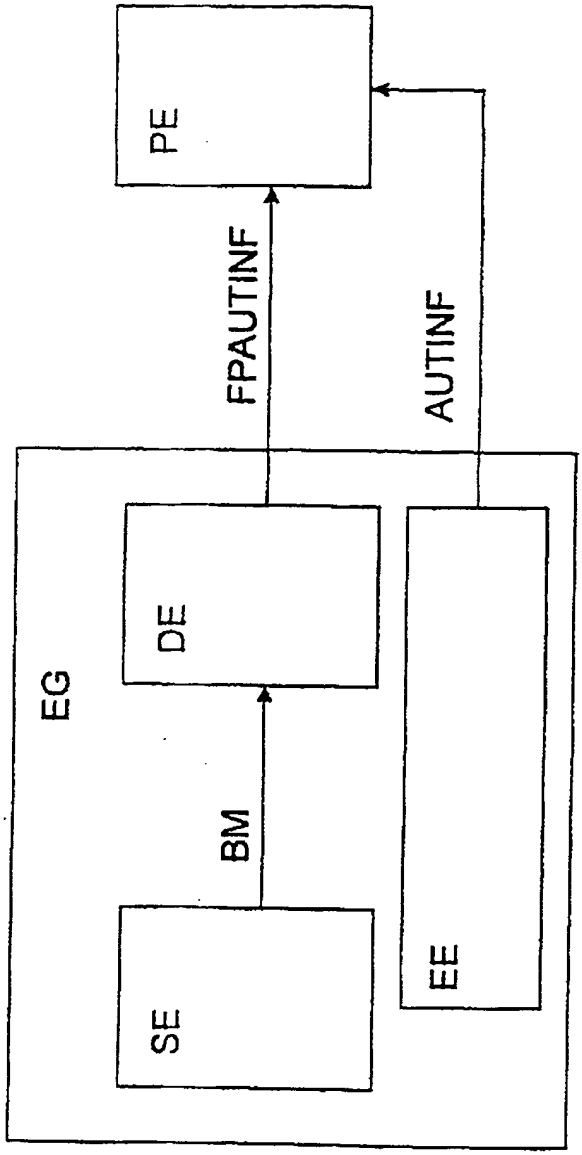
[Drawing 1]

FIG 1



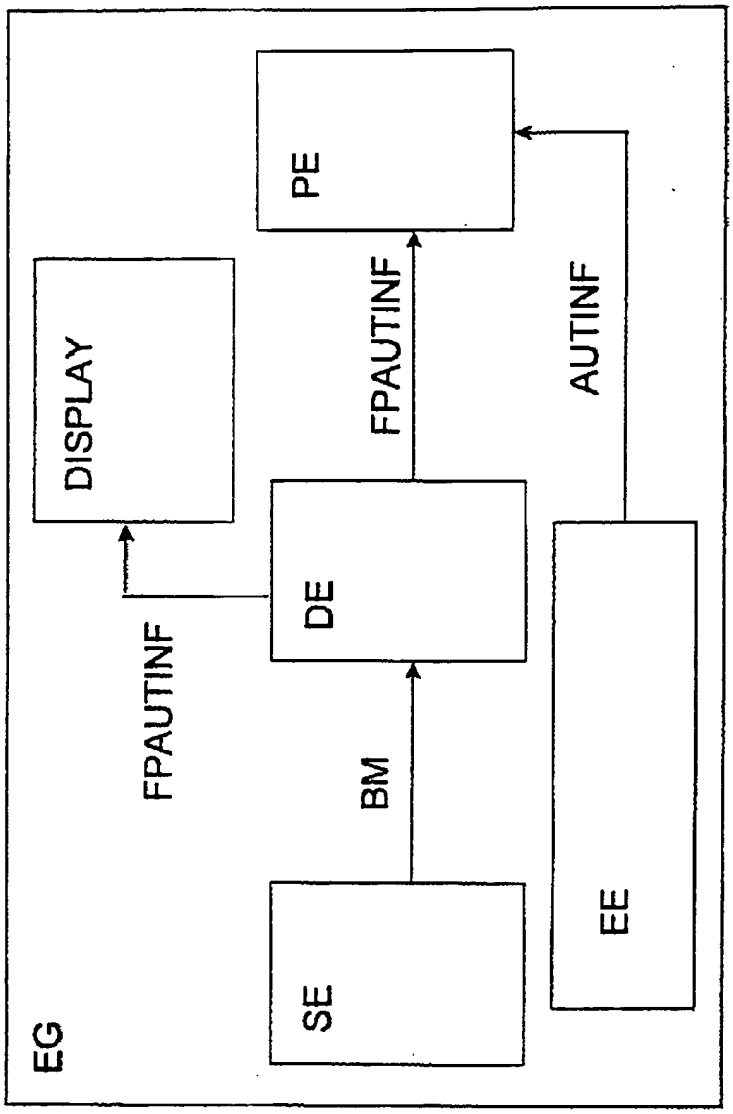
[Drawing 2]

FIG 2



[Drawing 3]

FIG 3



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2002－512409
（P2002－512409A）
(43)公表日　平成14年４月23日(2002.4.23)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｆ	５Ｂ０８５
Ｈ０４Ｑ　7/38		Ｈ０４Ｍ　1/66		５Ｋ０２７
Ｈ０４Ｍ　1/66		Ｈ０４Ｂ　7/26	１０９Ｍ	５Ｋ０６７
			１０９Ｒ	

審査請求　未請求　予備審査請求　有　（全 19 頁）

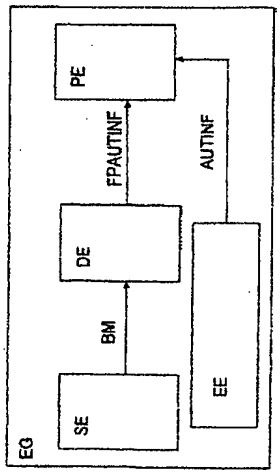
(21)出願番号　特願2000－545128(P2000－545128)
(86)(22)出願日　平成10年８月21日(1998.8.21)
(85)翻訳文提出日　平成12年10月20日(2000.10.20)
(86)国際出願番号　ＰＣＴ／ＤＥ９８／０２４５７
(87)国際公開番号　ＷＯ９９／５４８５１
(87)国際公開日　平成11年10月28日(1999.10.28)
(31)優先権主張番号　１９８　１７　７７０．４
(32)優先日　平成10年４月21日(1998.4.21)
(33)優先権主張国　ドイツ（ＤＥ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＣＹ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＢＲ，ＣＡ，ＣＮ，ＪＰ，ＫＲ，ＵＳ

(71)出願人　シーメンス　アクチエンゲゼルシヤフト
ＳＩＥＭＥＮＳ　ＡＫＴＩＥＮＧＥＳＥＬＬＳＣＨＡＦＴ
ドイツ連邦共和国　Ｄ－80333　ミュンヘン　ヴィッテルスバッハープラッツ　２
(72)発明者　クラウス－ペーター　カールマン
ドイツ連邦共和国　ミュンヘン　シュトラスベルガー　シュトラーセ　８
(74)代理人　弁理士　矢野　敏雄　（外４名）

Ｆターム(参考)　5B085 AE02 AE25 AE26
5K027 AA11 BB09 EE11 HH11 HH23 HH24
5K067 AA21 BB04 EE02 HH32 HH36

(54)【発明の名称】　電子機器、およびこの機器のユーザの認証を行う方法

(57)【要約】
機器は生理学的特徴ＢＭ（例えば指紋）を検出するセンサと、認証データＡＵＴＩＮＦ（例えばＰＩＮ）を入力する入力装置とを有している。この機器のデータ処理装置ＤＥは生理学的特徴ＢＭから認証情報ＦＰＡＵＴＩＮＦを求める。この情報は、入力装置ＥＥを介して入力される認証情報ＡＵＴＩＮＦと同じ検査装置ＰＥで検査される。これによりこの機器ＥＧを種々のユーザは生理学的特徴のためのセンサのない装置と同様に利用できる。認証プロトコル（例えば移動電話ではＳＩＭカード）を変更する必要はなく、これにより生理学的特徴による認証が可能となる。



【特許請求の範囲】

【請求項１】　電子機器、例えば情報処理または通信用の機器において、

ａ）機器のユーザの生理学的特徴（ＢＭ）、例えば指紋を検出するセンサ装置（ＳＥ）と、

ｂ）ユーザの認証に利用される情報（ＦＰＡＵＴＩＮＦ）を検出された生理学的特徴から求めるデータ処理装置（ＤＥ）と、

ｃ）情報を入力する入力装置（ＥＥ）、および該入力装置を介して認証に利用される情報（ＡＵＴＩＮＦ）を入力する手段と、

ｄ）求められたかまたは入力された認証情報を検査し、かつ検査が有効であった場合に当該のユーザに対して機器の機能を解放する検査装置（ＰＥ）とを有する、

ことを特徴とする電子機器。

【請求項２】　前記データ処理装置（ＤＥ）は、有効な認証の検査のために入力装置を介して入力される認証情報（ＰＩＮ）が権限を有するユーザの生理学的特徴から求められた認証情報（ＦＰＰＩＮ）と同一であるように構成されている、請求項１記載の機器。

【請求項３】　前記データ処理装置（ＤＥ）は検出されたユーザの生理学的特徴から当該のユーザの認証に利用される情報（ＦＰＡＵＴＩＮＦ１，．．．，ＦＰＡＵＴＩＮＦｎ）を求める複数のプロセス（Ｍ１，．．．，Ｍｎ）を使用できる、請求項１または２記載の機器。

【請求項４】　前記データ処理装置は権限を有するユーザに対して、生理学的特徴から認証情報を求める複数のプロセスのうち所望のプロセスを選択させる、請求項３記載の機器。

【請求項５】　ユーザの生理学的特徴から求められた認証情報（ＦＰＡＵＴＩＮＦ）を表示する手段を有する、請求項１から４までのいずれか１項記載の機器。

【請求項６】　ユーザはユーザに固有の生理学的特徴を用いてまたは認証情報を情報入力装置を介して入力することにより認証を行う手段を有しており、第１のケースではユーザの生理学的特徴をセンサ装置により検出し、検出された生

理学的特徴から認証に利用される情報を求めて検査装置により検査し、第２のケースではユーザが入力装置を介して入力した認証情報を同じ検査装置で検査する、

ことを特徴とする機器ユーザの認証を行う方法。

【請求項７】　ａ）センサ装置の測定データから特徴ベクトルを求めるステップと、

ｂ）求められた特徴ベクトルからベクトルを量子化するステップと、

ｃ）ベクトルの量子化の結果に対応する認証情報を検査するステップとを有する、

請求項６記載の機器ユーザの認証を行う方法。

【発明の詳細な説明】

【０００１】

利用する前にユーザが認証ないしオーセンティフィケーションを行わなくてはならないきわめて様々の電子機器が知られている。その主たる例は種々の構成のコンピュータ（情報処理機器）や通信機器、例えば移動電話などである。これらの機器には一般に不正使用に対して例えばパスワードにより保護されているものがある。他の機器は単に所定の機能のみを不正アクセスに対して（例えばいわゆる個人識別番号ＰＩＮによって）保護している。これには所定のデータまたはサービスへのアクセスの保護も属している。これが機器により使用されるのではなくてコンピュータネットワークまたは通信ネットワークにより使用される場合でもそうである。

【０００２】

今日頻繁に使用される形式の認証情報の入力は機器のキーボードを介した入力である。入力後に入力された情報の正当性、ひいては入力を行ったユーザの権限が機器またはコンピュータネットワークまたは通信ネットワークの検査装置で検査される。ＧＳＭ規格に準拠した移動電話では、これは機器のいわゆるＳＩＭカード上のデータ処理装置を用いて、入力されたＰＩＮがＳＩＭカードに記憶された情報に適合するか否かを検査することにより行われる。適合する場合にはＳＩＭカードにより移動電話が使用可能となる。ＧＳＭ規格に準拠してＰＩＮが機器内に記憶されず、ロックされた状態でＳＩＭカードに記憶されている場合、電話の顧客のセキュリティは上昇する。

【０００３】

しばらく前からユーザの認証を他の形式で行うことのできる技術が使用されている。この技術はユーザに固有の生理学的特徴を特別のセンサによって検出することに基づいている。この主な例は指紋検出センサである。別の生理学的特徴は例えば人間の目の網膜組織または人間の声の特性であり、これらも同様に数種の機器で使用されている。

【０００４】

通常はセンサによって検出された特徴は機器または通信ネットワークのデータ

処理装置で権限を有するユーザの既知の特徴と比較され、充分に一致する場合に所望のサービス、必要なデータまたは選択された機器の機能へのアクセスが解放される。

【０００５】

幾つかのタイプの機器では、前述の２つの形式の認証が相互に組み合わせると有意義である。例えば移動電話では、ユーザが指紋センサによって電話を利用できるだけでなく、ＰＩＮを他の人物とシェアしたり、固有のＳＩＭカードで機器を与えられている権限の範囲内で利用できるように利用できたりするほうが望ましい。さらに指紋を介した認証は偶発的にエラーを発生したり、または実行不能になったりする。これは例えばユーザの手が汚れていたり、ユーザが手袋を着けていたりする場合である。これらの理由またはその他の理由から望ましいのは（または必要なのは）、機器の１人または複数人のユーザが異なる手法で認証を行えることである。生理学的な認証はこのケースではＰＩＮ入力による認証と並んで行われる。ＧＳＭ規格に準拠する移動電話では、この規格がＰＩＮ入力による認証手段を強制的に予め定めている。

【０００６】

前述の状況から、従来の生理学的な認証プロセスはＧＳＭ規格に準拠する移動電話では不可能であることがわかる。なぜならＧＳＭ規格に対する互換性の理由から、ＳＩＭカードを用いたＰＩＮによる認証が必ず要求されるからである。さしあたり可能に見える手段として、ＰＩＮを機器内に記憶し、検出された指紋と権限を有するユーザの記憶された指紋と一致して検査が有効である場合に記憶されているＰＩＮをＳＩＭカードへ譲渡して検査することが考えられるが、これは排除される。なぜならＰＩＮを移動電話においてＳＩＭカード内部以外の別の場所に記憶することはセキュリティ上の理由からＧＳＭ規格により禁じられているからである。生理学的な認証はこの場合には付加的なセキュリティ手段として考慮される。ただしこのような付加的なセキュリティ手段はＰＩＮ入力による認証の高い安全性からすれば不必要であり、多くのユーザが受け入れがたく感じるはずである。

【０００７】

本発明の基礎とする課題は、生理学的なユーザの認証とＰＩＮ入力による認証との組み合わせをＧＳＭ規格または類似のケースの移動電話においても可能にし、それぞれの形式の認証を充分に活用できるようにする技術的思想を提供することである。ユーザはどちらの形式の認証を使用したいかという選択権を有している。ただし特に選択されたユーザ（例えば機器の所有者）が機器での２つの認証形式の論理ＡＮＤ結合を調整できる手段を有するようにすることもできる。この課題は特許請求の範囲に記載の機器または方法により解決される。

【０００８】

本発明では、ユーザの生理学的特徴がセンサ装置により検出され、検出された生理学的特徴から認証に利用される情報が数学的プロセスを用いて求められる。これにより生理学的特徴を評価する最終段階で認証情報が生じ、この情報はユーザが情報入力装置（例えばキーボード）を介して入力した認証情報を検査するのと同じ検査装置で検査される。最も簡単なケースでは指紋の評価の結果はユーザがキーボードを介して入力したＰＩＮと同じものとなる。ただしこのＰＩＮは機器に記憶されるのではなく、センサ装置によって検出されたユーザの生理学的特徴から計算される。

【０００９】

センサ装置によって検出された生理学的特徴を評価する形式により、この形式の認証はキーボードの入力を介した認証の結果と同等となり、認証の妥当性を検査する通常のインタフェースを変更しなくてもよくなる。特に規格化された何らかのプロトコルを変更する必要はない。認証の２つの手法は問題なく並列的に使用することができる。ユーザはいつでもどんな状態でも２つの手法を自由に選択できる。もちろんＡＮＤ結合を使用して２つの認証手法が有効に経過したユーザのみに許可を与えるように構成することもできる。

【００１０】

以下に本発明を有利な実施例に則して図を用いて詳細に説明する。

【００１１】

図１には、全ての方法および装置が機器内に集積されている本発明の実施例が示されている。

【００１２】

図２には検査装置が機器内に存在している本発明の実施例が示されている。

【００１３】

図３には認証情報を表示する表示装置が機器に集積されている本発明の実施例が示されている。

【００１４】

本発明に典型的でしかも重要な実施例はＧＳＭ規格に準拠する移動電話であり、これはユーザの認証に指紋センサを使用する。この指紋センサは図１に示されたセンサ装置ＳＥの特殊な例である。機器ＥＧのユーザが指をこの指紋センサに載せて、機器が例えばＰＩＮまたはＳｕｐｅｒＰＩＮまたはＰＩＮ２（部分的にメーカに依存する）などの入力の認証を行うのを待機していると、指紋センサが当該のユーザの相応の生理学的特徴ＢＭを検出し、これをデータ処理装置ＤＥへ送出する。

【００１５】

ＧＳＭ移動電話の場合、このデータ処理装置は移動電話に既に設けられているプロセッサと、このプロセッサ上で動作するソフトウェアとである。しかし他方では指紋センサは（または一般にセンサ装置は）固有のプロセッサユニットを介して使用され、このプロセッサユニット上で指紋認識を管理する特別のソフトウェアが動作する。これによりデータ処理装置は本発明の範囲では完全にまたは部分的にセンサ装置内に組み込まれている。指紋認識自体は生理学的特徴を認識する他の手法と同様に、データ処理装置の実現形態すなわち種々のコンフィグレーション（およびサブシステムでのパーティショニングまたは周知のハードウェアモジュールの統合）が当業技術者には充分に周知であるので、この部分に関しては本発明のセキュリティの実現に特に問題はない。

【００１６】

本発明によれば、データ処理装置は検出された生理学的特徴からユーザの認証に適した情報を求める。最も簡単なケースではこれは権限を有すると見なされるユーザのＳＩＭカード上にロックされた状態で記憶されたＰＩＮ（ないしＰＩＮ２その他）である。このＰＩＮはユーザが移動電話のキーボード（情報入力装置

）を介して入力したのと同様にＳＩＭカードへ引き渡され、検査される。次に当業技術者には周知のＧＳＭ規格に定められている検査過程が移動電話の検査装置（ＳＩＭカード、場合により機器のデータ処理装置と関連している装置）内で動作する。認証情報ＦＰＡＵＴＩＮＦが正しい場合、すなわちＳＩＭカード上に記憶されたＰＩＮと一致する場合には、認証により保護されている機器の機能（例えばネットワークアクセスなど）が解放される。

【００１７】

前述の本発明の手段の重要な利点は、ユーザが権限を有している場合に指紋認識部がユーザのＰＩＮをＳＩＭカードへ引き渡すことである。というのはこれによりＧＳＭ規格のセキュリティプロトコルを全く変更しなくて済むからである。他の基礎的と思われる手段にはこの有利な特性が存在しない。いずれにしろ他の手段ではキーボードを介した付加的なＰＩＮの入力が必要となるか、またはＧＳＭ規格の回避ないし変更が必要となる。キーボードを介した付加的なＰＩＮの入力は、指紋認識をＰＩＮ入力に加えた付加的なセキュリティ手段として考慮する場合にのみ有効である。

【００１８】

このような付加的な認証はもちろん本発明によっても可能である。この場合センサデータから求められた認証情報はＳＩＭカードへ伝送しなくてもよい。その代わりに例えば故意に誤ったＰＩＮをＳＩＭカードへ伝送してしまったり、または入力エラーまたは入力の中断その他などがシミュレートされたりすることがある。これに対してＳＩＭカードは新たにＰＩＮ入力を要求する。入力されたＰＩＮが求められたＰＩＮと一致するかまたは互換的である場合には、データ処理装置ＤＥはこのＰＩＮをＳＩＭカードへ伝送し、これに応じて解放が許可される。

【００１９】

もちろんセンサデータから求められたＰＩＮは必ずしもＳＩＭカードのＰＩＮと同一でない場合もありうる。前述の規格または他の機器ではそのつど適切なセキュリティプロトコルが許可する場合には、検査装置が２つの異なる認証情報によって、これらが相互に適合するか否かを検査することができる。

【００２０】

ＧＳＭ規格に準拠しない他の機器では、センサデータから計算された認証情報ＦＰＡＵＴＩＮＦがセンサデータによるただ１つの認証（すなわちＰＩＮ入力と同時の認証またはこれと独立の認証）で有る場合、キーボードを介して入力された認証情報ＡＵＴＩＮＦと異なっていることがあるが、２つの情報が権限を有するユーザを指示すれば、検査装置はこれらが同時に適合していると認識する。

【００２１】

生理学的特徴ＢＭから得られた認証情報ＦＰＡＵＴＩＮＦに対する計算プロセスとして基本的に全ての数学的なシミュレーション（関数）が考慮され、指紋または他の生理学的特徴ＢＭに他の形式の（一般には英数字によって符号化された）認証情報ＡＵＴＩＮＦが割り当てられる。ここで次の条件を満足しなければならない。すなわち

ａ）充分に類似の生理学的特徴ＢＭから同じ認証情報ＦＰＡＵＴＩＮＦが導出され、

ｂ）充分に異なる生理学的特徴ＢＭから異なる認証情報ＦＰＡＵＴＩＮＦが導出され、

ｃ）不正のユーザにとっては、認証情報ＦＰＡＵＴＩＮＦを生理学的特徴ＢＭまたはこの特徴ＢＭの知識から求める（例えば推測する）ことが実質的に不可能である、

ことである。

【００２２】

条件ａ）は指紋認識が小さなノイズに対しても充分にロバストで有ることを保証する。そうでないと権限を有するユーザが拒絶される割合がきわめて高くなってしまうからである。条件ｂ）はこれに対して、異なるユーザの指紋が充分に高い確率で種々の認証情報ＦＰＡＵＴＩＮＦを導出するように設けられている。条件ｃ）の意義は明らかである。

【００２３】

当業者には（場合によって適切さの多少はあるが）この要求を満足する種々の数学的シミュレーションが周知である。これらの特性を有するシミュレーションはいわゆるベクトル量子化によって与えられる。当業者に周知の手法については

ここでは本発明の理解に必要であると思われる個所以外は説明しない。

【００２４】

この手法を本発明の目的に使用する際にはまず、センサ装置によって検出された生理学的特徴がいわゆる特徴ベクトルの形式へ移されることを前提とする。この仮定は実際には何らの限定にもならない。なぜならセンサデータはつねにｎ個の測定データ（特徴ベクトル）の順序づけられたｎ個のグループとして表されるからである。特徴ベクトルはｎ次元の空間を形成する。この空間内にはパターンベクトルの集合（コードブックベクトル）が存在し、距離尺度（生理学的特徴に対する類似の度合）が規定される。各パターンベクトルに対して空間内のセルが存在し、このセルはセル内の各特徴ベクトルに相応し、パターンベクトルは当該の距離尺度の範囲内で次に存在するパターンベクトルのセルであることにより規定されている。

【００２５】

各パターンベクトルには認証に基本的に適した情報が割り当てられている。１つのパターンベクトルには正確な認証情報（例えば真のＰＩＮ）が割り当てられている。前述の説明から明らかなように、検出されたセンサデータに相応する所定の特徴ベクトルに対して次に存在するパターンベクトルを求めると、当該のユーザが権限を有する場合には正確な情報（真のＰＩＮ）が導出され、そうでない場合には誤った認証情報が送出される。このプロセスのエラーレートは権限を有するユーザの生理学的特徴に関連する特徴ベクトルがパターンベクトルの１つであることが保証される場合に最適化することができる。これはこのシステムを初期化フェーズで権限を有するユーザの生理学的特徴に適応させること（コードブック適応化）により達成される。

【００２６】

ベクトル量子化は本発明に関連して使用できる唯一の手法ではない。当業者にはここで説明しない他の手法も実施可能である。

【００２７】

認証情報ＦＰＡＵＴＩＮＦをユーザの生理学的特徴からベクトル量子化により計算することは（本明細書に基づくならば）本来機器での“ＰＩＮの記憶”に結

びついている。なぜならコードブックの各パターンベクトルには基本的に可能な認証情報ＦＰＡＵＴＩＮＦが割り当てられているからである。ただしこれはほぼ全てのケースで（１人のユーザ、すなわち権限を有するユーザの特徴ベクトルを除いて）実際には認証には適さない。つまり例えば５桁の英数字のＰＩＮでは理想的には全ての可能なＰＩＮが記憶されてこれらのそれぞれに１つずつパターンベクトルが割り当てられるのであるが、パターンベクトルが充分に正確に検出された場合にしかセンサ内で妥当なＰＩＮにアドレシングできない。したがって正確なＰＩＮは“機器内に記憶されている”にもかかわらず、可能なＰＩＮの数が大きくなりすぎ、正確な生理学的特徴を有するユーザ以外は見いだせなくなってしまうのである。こうした状況は規格によってＰＩＮを機器に記憶することが禁止されている場合には考慮されていない。

【００２８】

ＧＳＭ規格ではＰＩＮを機器に記憶することは許可されていない。ただしＰＩＮを変更する必要は頻繁に生じる。これは例えばＰＩＮが第３者に知られてしまった場合などである。ただし本発明ではＰＩＮを指紋から求める（すなわち計算する）ので、指紋または他の生理学的特徴の交換が可能でないかぎりこれはまず不可能である。それでもユーザにＰＩＮを変更する手段を与えるのであれば、本発明の有利な実施形態により、ただ１つの計算プロセスに代えて機器内のこの種のプロセスの全ての集合を同等に使用できるように構成する。個々の計算プロセスには連続番号が割り当てられており、これに対して権限を有するユーザは使用するプロセスをいつでも変更できる。同一の指紋ＢＭに対する各プロセスＭ１，．．．，Ｍｎは他のＰＩＮ（ＦＰＡＵＴＩＮＦ１，．．．，ＦＰＡＵＴＩＮＦｎ）を計算するので、ユーザは多数のＰＩＮをどのプロセスで計算させるかを選択する。

【００２９】

本発明の実施例は同様にベクトル量子化によっても実現できる。ここでコードブックだけでなく、パターンベクトルの複数のコードブックも設けられている。各コードブックは所定の番号を有しており、この番号を介して選択可能である。他のプロセスはおそらくパラメータに依存している。本発明ではこのパラメータ

を変更することにより、他の数学的なシミュレーションも形成する。パラメータの依存性が充分に複雑であれば、実際にはパラメータを変更しても認証情報の変更は推測が不可能になる。所定のタイプのニューラルネットワーク（いわゆるマルチレイヤパーセプトロン）はこの種のシミュレーションを実現するのに適してる。このニューラルネットワークに基づく手段ではＰＩＮは実際にはどこにも記号シーケンスとしては記憶されておらず、単に（暗示的にロックされた状態で）ネットワークアーキテクチャに重みづけ係数として記憶される。

【００３０】

本発明のこの実施例では、特に多数の人物の異なるパスワードのシーケンスが完全に異なる目的または機器に対して必要となる観点から考慮される。多数のパスワードに留意することはますます困難となるはずである。複数のプロセスＭ１，．．．．，Ｍｎ（数学的シミュレーション）を複数の認証情報（ＦＰＡＵＴＩＮＦ１、ＦＰＡＵＴＩＮＦ２）の唯一の特徴ベクトル（センサデータの集合）からの計算に使用する場合、ユーザに固有の公けにできない生理学的特徴を検出する際の問題が適切なセンサにより低減される。

【００３１】

所定のプロセスを選択するためには、単にユーザの操作表面に設けられたコンテクストでこの種のプロセスのインデクスを入力すればよい。これによりソフトウェアごとにデータ処理装置が相応に構成できる。

【００３２】

もちろん複数の人物の生理学的特徴を１つまたは複数の正しいＰＩＮと結合することもできる。機器が例外として１人の人物としか結合されていない場合、すなわち正確に１つのＳＩＭカードしか使用されない場合には、解放は付加的に他のセキュリティ機構、例えば機器のコードなどに結合できる。本発明によればここではそれぞれの形式の柔軟性と高い安全性、規格に対する互換性が得られる。

【００３３】

ＰＩＮを変更する場合、本発明の特に有利な別の実施例では、認証情報の表示用のディスプレイが設けられている。この種のディスプレイはこの種の多数の機器ですでに始めから存在しているので、これをこの目的のために利用できる。ユ

ーザがキーボードを介して入力した認証情報ＡＵＴＩＮＦ（例えばＰＩＮ）をＳＩＭカードに適合する情報に変更しようとすると、幾つかの計算プロセスでは場合により可能な全ての記号の数字の組み合わせがＰＩＮとして使用できない。なぜなら例えばコードブックが可能な全てのＰＩＮの数よりも小さいからである。このケースでは使用される計算プロセスのパラメータの変更（例えばコードブック番号の変更、またはニューラルネットワークのパラメータの変更）を行えば、ＰＩＮをパターンベクトルに割り当てて個人のパターンベクトルに対応するＰＩＮを変更するには充分である。その後はＳＩＭカード上のＰＩＮ（または一般に入力すべきＰＩＮ）を知らなければこの意味では変更できなくなる。しかもこれは本発明の課題に対する更なる利用のために必要である。変更されたＰＩＮは権限を有するユーザには有利には相応にＰＩＮを変更後に機器のディスプレイに１回だけ短時間表示させることにより知らせることができる。他の手段（例えば新たなＰＩＮを後から提示すること）も可能である。

【００３４】

本発明はもちろん移動電話、例えばＧＳＭ規格に準拠する移動電話に限定されるものではない。当業者には前述の説明に基づいて、本発明を他の機器または他のシステムにおいて実現することも困難ではない。

【００３５】

特に本発明は検査ユニットＰＥが機器内に集積されているケースのみに限定されない。図２には機器の重要な例が示されており、ここでは機器は例えば通信ネットワークを介して少なくとも１つの他の機器と接続され、検査装置もネットワーク内に存在している。またデータ処理装置またはデータ処理ユニットＤＥの一部、すなわちユーザの生理学的特徴ＢＭから認証情報ＦＰＡＵＴＩＮＦを計算することを管理する部分も必ずしも機器内に存在していなくてもよい。もちろん機器は集積されたセンサ装置ＳＥまたは集積されたキーボードＥＥを有していなくてもよい。装置を外部モジュールのかたちで機器に接続してもよいことも明らかである。本発明の実施例は方法の請求項により保護されるべきである。

【図面の簡単な説明】

【図１】

全ての方法および装置が機器内に集積されている本発明の実施例を示す図である。

【図２】

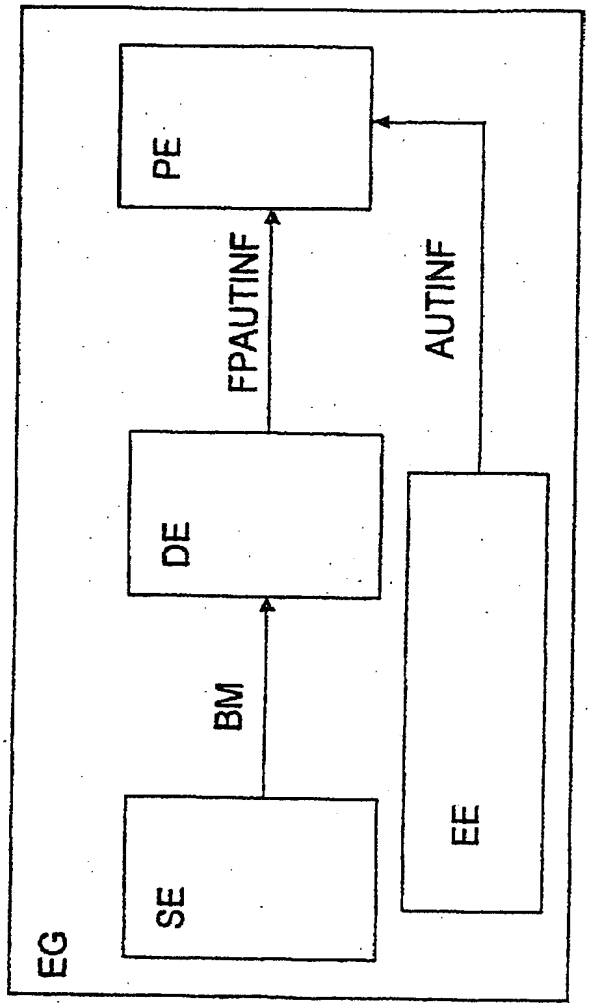
全ての方法および装置が機器内に集積されている本発明の実施例を示す図である。

【図３】

認証情報を表示する表示装置が機器に集積されている本発明の実施例を示す図である。

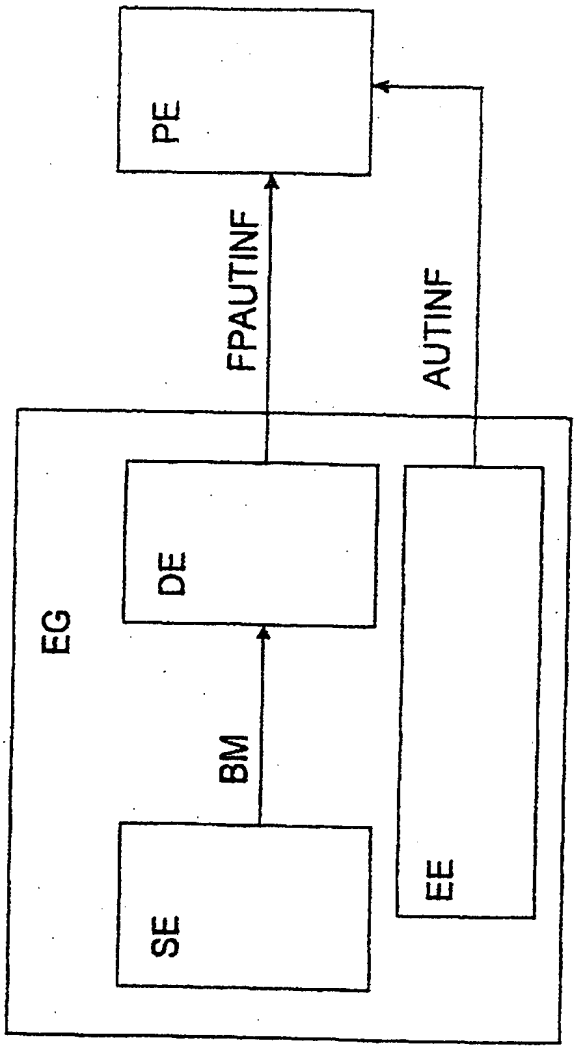
【図１】

FIG 1



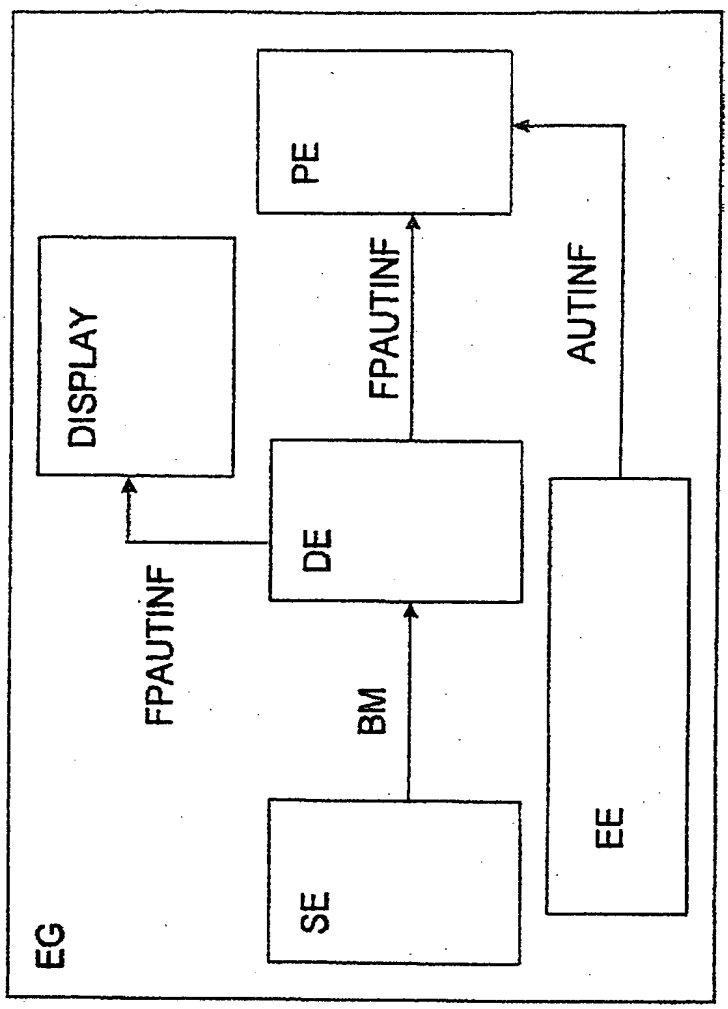
【図２】

FIG 2



【図３】

FIG 3



【国際調査報告】

INTERNATIONAL SEARCH REPORT

Int dional Application No
PCT/DE 98/02457

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07C9/00 H04Q7/38 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07C G07F H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 11750 A (SUBBIAH SUBRAMANIAN ;LI YANG (US); RAO D RAMESK K (US)) 19 March 1998 see page 3, line 8 - page 4, line 29 see page 5, line 34 - page 8, line 24; figures	1,3
Y		2,6
Y	DE 25 33 699 A (SIEMENS AG) 10 February 1977 see page 3, line 1 - line 12 see page 5, line 1 - line 7; figures; examples	2,6

-/—

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 January 1999	03/02/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Meyl, D

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int. ional Application No
PCT/DE 98/02457

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 731 426 A (JOHNSON NELDON P) 11 September 1996 see abstract; figures see column 5, line 7 - line 39 see column 6, line 36 - column 7, line 31	1,2,6
A	EP 0 504 616 A (ASCOM AUTELCA AG) 23 September 1992 see abstract; claims; figures	1-3,6
A	WO 96 08093 A (MYTEC TECHNOLOGIES INC) 14 March 1996 see abstract; figures see page 3, line 2 - line 18	1,2,6
A	WO 97 04375 A (SIEMENS AG OESTERREICH ;FORER JOSEF (AT); KAUF OTTO (AT)) 6 February 1997	
A	DE 93 04 488 U (SIEMENS AG) 29 July 1993	

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int ional Application No
PCT/DE 98/02457

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9811750 A	19-03-1998	AU 4341797 A	02-04-1998
DE 2533699 A	10-02-1977	NONE	
EP 0731426 A	11-09-1996	US 5598474 A	28-01-1997
		AU 693655 B	02-07-1998
		AU 4805096 A	19-09-1996
		BR 9600961 A	30-12-1997
		CN 1137659 A	11-12-1996
		JP 9114986 A	02-05-1997
EP 0504616 A	23-09-1992	NONE	
WO 9608093 A	14-03-1996	US 5541994 A	30-07-1996
		US 5680460 A	21-10-1997
		AU 689946 B	09-04-1998
		AU 3339095 A	27-03-1996
		BR 9509002 A	02-06-1998
		CA 2199034 A	14-03-1996
		CN 1157677 A	20-08-1997
		EP 0780040 A	25-06-1997
		JP 10505474 T	26-05-1997
		US 5737420 A	07-04-1998
		US 5832091 A	03-11-1998
WO 9704375 A	06-02-1997	EP 0782724 A	09-07-1997
DE 9304488 U	29-07-1993	NONE	